Welcome

The objective of the Annual Security Refresher Briefing is to remind individuals of their safeguards and security responsibilities and to promote continuing awareness of good security practices.

US Department of Energy (DOE) Order 470.4B Appendix B, Section 3 "***Safeguards and Security Awareness***" requires that individuals who possess DOE access authorizations shall receive refresher briefings to reinforce and update awareness of safeguards and security policies and their responsibilities. Refresher briefings are mandatory for all individuals possessing DOE access authorizations and shall be implemented each calendar year at approximately 12 month intervals.

About the Briefing

This Annual Security Refresher Briefing is divided into seven (7) sections. Upon completion of each section, a brief question and answer session will appear. Correct answers will be provided as you move forward. At the end of the briefing, a Briefing Summary Record will be emailed to you and the appropriate security official.

Section 1: Security Badges and Identification of Prohibited and Controlled Articles

Section 2: Reporting Requirements and Incidents of Security Concern (IOSC)

Section 3: Classified Information

Section 4: Technical Surveillance Countermeasures (TSCM), Operations Security (OPSEC) and Cyber Security

Section 5: Unclassified Controlled Information (UCI)

Section 6: Hosting Foreign National Guests

Section 7: Counterintelligence

Additional Features:

<u>Resource Library:</u> The Resource Library provides an acronym list and links to documents and web sites referenced throughout this briefing. Select the Resource Library icon at any time during the briefing to view and/or print useful information.

<u>Technical Support:</u> Provides contact information for each site's Information Technology Help Desk.

Can I open the Resource Library while I'm taking the course?
Yes! Opening the library won't interrupt your progress. The Resource Library contains phone ✓ lists, web site links & more.

What if I'm called away while taking the course?
This course will timeout after 30 minutes of inactivity. When you resume, just login and the course will pick up where you left off.

Section 1: Security Badges and Identification of Prohibited and Controlled Articles

The purpose of this section is to recognize the various security badges and your reporting responsibilities as it pertains to your badge. In addition, there is a review of Prohibited and Controlled Articles.

Security Badges

Your badge must be replaced or reissued if:

- Your name changes or your physical appearance changes.
- Your badge is faded or damaged.
- Your contract company changes.

Badge cautions:

- It is illegal to counterfeit, alter, or misuse your badge.
- **DO NOT** allow your badge to be photographed.
- **DO NOT** wear the badge in public places.
- Report the loss or theft of your badge immediately or within 24 hours.

Other badge reminders:

- Protect your badge from theft when you are offsite.
- Your badge is the property of DOE and must be returned to the Badge Office if it has expired, is no longer required, or upon termination of employment.

Prohibited Articles

Based on federal laws, regulations, and DOE directives, there are articles prohibited on DOE property.

The following articles are prohibited:

- Dangerous weapons and explosives (instruments or materials likely to cause substantial injury to people or damage property). This category includes pocket, hunting, or other sharp knives with blades 2.5 inches or longer.

- Non-government-owned firearms (even if you have a gun carry permit).

- Alcoholic beverages.

- Controlled substances such as illegal drugs and associated paraphernalia (but not prescription medicine).

- All items that are prohibited by law.

Controlled Articles

The following are controlled articles:

- Personal Data Assistants (PDA)s
- Personal laptop or palmtop computers
- BlackBerry devices
- Two-way pagers
- Cell phones
- Cameras of all kinds
- Recording equipment
- Digital audio players (iPod, Zune)
- Thumb and portable hard drives and most gaming devices (check with security)

The above articles are not allowed in Limited Areas, Exclusion Areas, Protected Areas, Material Access Areas, or other sensitive areas as designated by the facility, without authorization from the Cognizant Security Authority. **Check signs on buildings about controlled items.**

You may be able to use a controlled item outside a building, but not take it into the building. If you are uncertain, then do not introduce the items into the facility. Remember, introduction of any excluded controlled article into the above areas may result in a security infraction and result in an Incident of Security Concern reportable to DOE. Authorization for use of such devices in one security area does not apply to all other security areas.

Worker Responsibilities for Prohibited and Controlled Articles

ALL workers are responsible for reporting the unauthorized possession and use of prohibited and controlled articles.

Section 1: Security Badges and Identification of Prohibited and Controlled Articles Quiz

1. The following articles are prohibited on DOE property.

    a. Alcoholic beverages
    b. Controlled substances such as illegal drugs and associated paraphernalia
    c. Non-government-owned firearms (even if you have a gun carry permit)
    d. All of the above

2. The following items are controlled articles.

    a. Digital audio players
    b. Cell phones
    c. Cameras of all kinds
    d. All of the above

Section 2: Reporting Requirements and IOSC

When you completed your original Questionnaire for National Security Positions (QNSP) or Electronic Questionnaire for Investigative Process (e-QIP) and when a renewal of your clearance was requested, you were made aware of your responsibility to report certain personal information. Those reporting responsibilities are ONGOING**.**

Individual Reporting Requirements:

Remember that whether an individual (employee, contractor, subcontractor, etc.) holds a clearance or is in the process of obtaining a clearance, he or she is **required** to report certain personal information.

This information is to be reported within 2 days by phone and 3 days by written notification, unless noted otherwise, to the Personnel Security Office at your site.

Personnel Security Office telephone numbers are listed in the Resource Library.

Reporting Requirements

- **Arrests**
  Report all arrests, including charges that are dismissed.
- **Criminal Charges**
  Report all criminal charges including felony, misdemeanor, public and petty offenses as defined in the statutes of any state.
- **Detention by Law Enforcement**
  Report any detention by federal, state or other law enforcement authority for violation of law. The only exception to this reporting requirement is detention for a simple traffic stop.
- **Traffic Violations**
  Report any traffic violations for which you receive a fine of $300 or more unless the traffic violation is alcohol or drug related. **Any traffic violation that is alcohol or drug related must be reported regardless of the amount.**
- **Ongoing Contact with Foreign Nationals**
  Report employment, business and personal related associations with any foreign national or employees/representatives of a foreign-owned interest.

- **Hospitalization**
  Report hospitalization for treatment of mental illness or other mental condition; treatment for alcohol or drug abuse; any condition that may cause a significant impairment in judgment or reliability.
- **Bankruptcy**
  Report any personal or business-related bankruptcy.
- **Wage Garnishment**
  Report all wage garnishments including, but not limited to, divorce, delinquent debts, or child support.
- **Change in Marital/Cohabitation Status**
  Report marriage or cohabitation within 45 days.
- **Name Changes**
  Report all legal name changes.
- **Change in Citizenship**
  If you are a US citizen who changes citizenship or acquires dual citizenship, you must report this change to Personnel Security.
- **If an immediate family member assumes residence in a sensitive country.**

This information is to be reported within 2 days by phone and 3 days by written notification, unless noted otherwise, to the Personnel Security Office at your site.

General Security Reporting Requirements

You are also required to report immediately, upon discovery, incidents of security concern (IOSC), when you become aware that Classified Matter or Unclassified Controlled Information (UCI) has been, or may have been, lost or compromised, in person or by secure phone. Waste, fraud, and abuse, whether a crime is involved or not, must be reported to the site Security Office, Internal Auditing, or the Inspector General. Any damage to a DOE facility or theft of DOE property must be reported to the Inspector General.

Telephone numbers are listed in the Resource Library.

Incidents of Security Concern

An IOSC occurs any time there is a potential or actual compromise of classified or UCI or when a security rule is violated. IOSCs are actions, inactions, or events that have occurred at a site that:

- Pose threats to national security interests and/or critical DOE assets.
- Create potentially serious or dangerous security situations.
- Potentially endanger the health and safety of the workforce or public (excluding safety related items).
- Degrade the effectiveness of the safeguards and security program.
- Adversely impact the ability of organizations to protect DOE safeguards and security interests.

Remember, if you observe, find or have knowledge of or information regarding an IOSC, you must immediately report it to your site Security Office or site Shift Superintendent Office in person or by secure means. If you discover a potential IOSC, you must take reasonable and prudent steps to contain the incident, protect the scene, and secure classified and UCI matter, as appropriate.

IOSC telephone numbers are listed in the Resource Library.

Section 2: Reporting Requirements and IOSC Quiz

1. Which of the following events are reportable within 2 working days of the event?

   a. Detention by law enforcement for a simple traffic violation.
   b. Traffic violations for which you receive a fine of $100 or less.
   c. Arrests, criminal charges, bankruptcy.
   d. Use of over-the-counter medications.

2. Marriage or cohabitation with a person in a spouse-like relationship must be reported within 45 days.

   a. True
   b. False

3. Waste, fraud and abuse only has to be reported if a crime is involved.

   a. True
   b. False

4. When does an "incident of security concern" occur?

   a. Any time there is a potential or actual compromise of classified or UCI, or when a security rule is violated.
   b. Any time security personnel are in your building.
   c. All of the above.

Section 3: Classified Information

This section is to refresh your memory on Classified Information.

Subtopics to be reviewed are:

- Classification
- Levels and Categories of Classified Matter
- Access to Classified Matter
- Declassification and Downgrading
- Protection and Control Measures

Classification

Classification is the identification of information that needs to be protected in the interest of national security.

- Information regardless of physical form or characteristics is considered classified if it requires protection against unauthorized disclosure in the interest of national security.
- Classified matter is any combination of documents or material containing classified information.
- Classified information may only be shared or communicated in a location approved for classified discussions. Classified information may also be shared by approved secure/classified means. Examples of secure/classified means would be using a secure telephone for phone calls or a secure fax for data transmissions.

All classified information/material is protected according to federal statutes and Presidential Executive Orders. DOE is responsible, under the Atomic Energy Act of 1954, as amended, for classifying information and material relating to atomic energy and its use in weapons and under Executive Orders for other aspects of national security. The Atomic Energy Act of 1954 and Executive Order 13526 govern classification policy as implemented through 10 CFR 1045 and DOE Order 475.2A.

Classifying establishes protective barriers that ensure that classified information and material do not fall into unauthorized hands. Through the process of classification, we protect important information from adversaries, yet allow the same information to be used by scientists, statesmen, military planners, and others with applicable access authorization and who meet the need-to-know criterion.

Classification and Your Responsibilities

Documents or material potentially containing classified information must be reviewed for classification to ensure that such information is identified for protection.

Required Classification Reviews:

1. Newly generated documents or material in a classified subject area and that potentially contain classified information must receive a classification review by a Derivative Classifier (DC).
2. Existing unmarked documents or material that an employee believes may contain classified information must receive a classification review by a DC.
3. Existing documents or material that an employee believes may contain information classified at a higher level or more restrictive category must receive a classification review by a DC.
4. Documents or material in a classified subject area intended for public release (e.g., for a webpage, Congress) must be reviewed by a Classification Officer.
5. Newly generated documents that contain extracts from an existing classified document (e.g., a chapter or appendix) must be reviewed by a DC. If the extract is intended to be a stand-alone, unclassified document, then an additional review by a Derivative Declassifier (DD) is required.

Derivative Classifiers

DCs are knowledgeable in their technical fields, trained and certified to recognize classification issues. Per DOE policy, classification decisions (appropriate classification level, category, and required caveats) are made by the appropriately certified DC. Failure to have electronic documents properly marked, protected and reviewed for classification prior to distribution is one of the most common security infractions and results in an IOSC reportable to DOE.

When it is reasonable to expect that documents or materials contain classified information or when regulations or other requirements apply, you are personally responsible to ensure the matter is reviewed by an approved DC or the site Classification Officer. These individuals are authorized to determine the highest classification level and category of the information provided in the matter.

Classification Officers and Classification points of contact for each site are listed in the Resource Library.

Levels of Classified Information

Classified information is designated by both a classification level and a category.

The classification **level** is based on how much our national security could be damaged if the information were to be released to unauthorized person (s).

There are three classification levels:

- **Top Secret** information can be expected to cause exceptionally grave damage to national security.
- **Secret** can be expected to cause serious damage to national security.
- **Confidential** can be expected to cause damage to national security.

Categories of Classified Information

The classification **category** describes the type of information contained in the material.

There are three classification categories:

- **Restricted Data** is information that is related to the design, manufacturing, and utilization of atomic weapons; production of special nuclear material; or use of special nuclear material in the production of energy.
- **Formerly Restricted Data** is information that pertains to the military utilization of atomic weapons and has been removed by DOE from the Restricted Data category.
- **National Security Information** is information that requires protection in the interest of national defense or foreign relations of the United States that is not related to nuclear weapon design, manufacturing, testing, or utilization.

Access to Classified Information

The following table depicts the classification levels and categories of information individuals are authorized to access based on their clearance:

	Restricted Data	Formerly Restricted Data	National Security Information
Top Secret	**Q**	**Q**	**Q**
Secret	**Q**	**Q** or **L**	**Q** or **L**
Confidential	**Q** or **L**	**Q** or **L**	**Q** or **L**

Access to classified matter must be limited to persons who possess appropriate access authorization, have a need to know for the performance of official duties, and have signed an SF-312 (Classified Information Non-disclosure Agreement).

Access is not obtained or granted by position only.

Access to Classified Information

Classification Challenge

Although authority for making classification determinations rests with a DC, each employee is encouraged and expected to challenge the classification of information, document or material that he or she believes is improperly classified. Challenges should be directed to your site Classification Office.

Declassification

Declassification is the determination that classified information (document or material) no longer requires, in the interest of national security, any degree of protection against unauthorized disclosure, together with removal or cancellation of the classification designation.

(In most cases only a Derivative Declassifier may remove markings from a classified document.)

Declassification and Downgrading

If you believe currently marked classified matter should be declassified or downgraded (you believe the information belongs in a lower classification level or category), contact a Derivative Declassifier, or the Classification Office at your site.

A Derivative Classifier (DC) is not authorized to ***declassify*** classified matter.

Protection and Control Measures

No Comment Policy

The fact that DOE classified information has appeared publicly (in newspapers or magazines) does not make it unclassified. Therefore, you must respond "no comment" to any questions about the accuracy, classification, or technical merit of such information.

Unauthorized Disclosure

- A communication or physical transfer of classified matter to an unauthorized recipient.
- Could potentially cause damage or irreparable injury to the US, or could be used to advantage by a foreign nation.
- Can occur when an individual intends to transfer classified matter or by negligent handling.

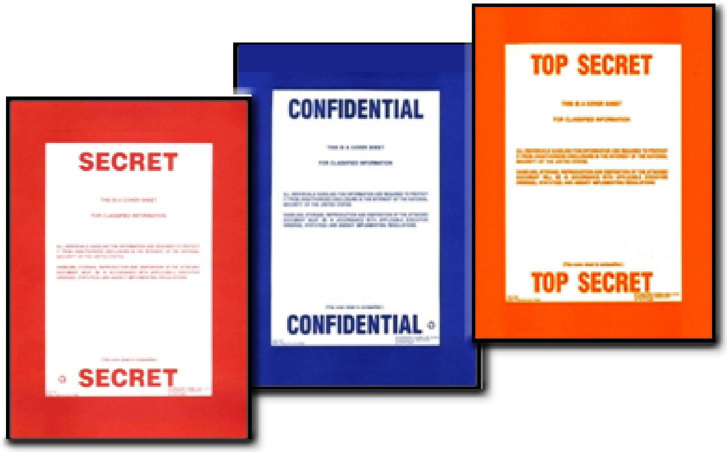
Penalties for unauthorized disclosure

- Termination of Security Clearance
- Removal from any position of special confidence and trust requiring clearance
- Termination of employment
- Punishment under criminal sanctions
- Monetary fines

Protection and Control Measures

Cover sheets must be used any time a classified document is removed from a repository (sometimes referred to as a safe), vault, or vault-type room. The purpose of a classified cover sheet is to prevent unauthorized visual access, serve as an immediate identifier that the attached document or material is classified, and identify the classification level of the document.

Classified cover sheets are identified as follows:



For additional protection and control measures, including training/briefing requirements, contact the site Classified Matter Protection and Control (CMPC) point of contact (POC).

Contact information listings can be found in the Resource Library.

Accountable Classified Matter

Certain classified matter (i.e., paper, electronic, parts) requires stricter controls to prevent unauthorized access to or removal. These controls include a system of procedures that provide an audit trail and a chain of custody.

Classified matter requiring a control system and accountability is:

- Top Secret matter.
- Secret Restricted Data matter, or higher, stored outside a Limited Area (LA).
- National, International, or programmatic requirements such as:
    - Atomic Coordinating Office/United Kingdom (ACO/UK).
    - North Atlantic Treaty Organization (NATO).
    - Top Secret and Secret Foreign Government Information.
- Communications Security (COMSEC) keying material such as Cryptography (CRYPTO).
- Special Access Programs (SAP).
- Sigma 14.

Section 3: Classified Information Quiz

1. Classified matter is structured into which three categories?

   a. Top Secret, Secret, Confidential
   b. National Security Information, Formerly Restricted Data, Restricted Data
   c. Confidential Information, Top Secret information, National Security Information

2. Documents or material in a classified subject area intended for Congress does not have to be reviewed by a DC.

   a. True
   b. False

3. What must an individual possess before being allowed access to classified matter?

   a. An "L" or "Q" clearance.
   b. The need to know and at least an "L" clearance
   c. Appropriate access authorization, need to know, and a signed Classified Information Non-disclosure Agreement (SF-312).

4. The classification levels are:

   a. Top Secret
   b. Secret
   c. Confidential
   d. All of the above

Section 4: Technical Surveillance Countermeasures (TSCM), Operations Security (OPSEC) and Cyber Security

This section will review:

- **the TSCM Program, reporting requirements, and points of contact.**
- **the OPSEC Program, reasons for the program, and the importance of your participation in the program.**
- **Cyber Security requirements and the reasons to be wary of suspicious emails.**

Technical Surveillance Countermeasures

TSCM is a counterintelligence program that is designed to detect, deter, isolate, and nullify the technologies that are intended to obtain unauthorized access to classified and unclassified controlled information and range from simple mechanical to sophisticated electronic and fiber-optic techniques. The more common techniques include hidden audio and Radio Frequency (RF) transmitting devices (microphones), telephone bugging equipment, and visual tools such as binoculars, telescopes, mini cams, and fiber optic cameras. The sale of these devices is not restricted. They are readily available to anyone on the commercial market.

- If you discover what you consider a technical surveillance device, you should, as discreetly as possible, immediately cease all activity in the area.
- Do not voice the discovery within the immediate area, which includes the suspect room and all other rooms that are above, below, and adjacent to it.
- **<u>Secure the room and do not touch or remove the device.</u>**
- Immediately notify your TSCM point of contact via secure communications, outside of the area where the suspected device has been found. During off-shift hours notify the Oak Ridge Operations Center (OROC) or site Shift Superintendent's Offices.

Note: Any action related to TSCM information or possible vulnerability should be protected as classified information.

The TSCM points of contact are listed in the Resource Library.

Operations Security

OPSEC is an analytic process used to deny an adversary information - generally unclassified - concerning friendly intentions and capabilities by identifying, controlling, and protecting indicators associated with planning processes or operations.

<u>OPSEC does not replace other security disciplines - it supplements them</u>.

The principles of OPSEC are based on asking five questions:

1. **What information do you want to protect?**
2. **Who wants your information?**
3. **How is your information vulnerable?**
4. **What is the risk for your information?**
5. **How can you protect your information?**

OPSEC: How can I do my part?

- Use passwords to access your government computers.
- Destroy UCI by approved methods.
- Do not transmit sensitive information without following proper security procedures.
- Do not discuss UCI or classified information in public.
- Limit distribution of UCI (need-to-know).
- Guard against phone calls seeking personal and sensitive information.
- Use appropriate markings on UCI and classified correspondence.
- Watch for possible inadvertent ways in which we release information.
- Be aware of possible ways in which an adversary can collect information in an open environment (e.g., overheard conversations, notes left in open vehicles, etc.).
- Practice need-to-know.
- Use encryption/VPN.

Cyber Security

The Information Technology (IT) Program establishes requirements for protecting DOE information and information systems. These requirements include provisions for ensuring that the protection is commensurate with the risk and damage that could result from the loss, misuse, disclosure, or unauthorized modification of information that is processed, stored or transmitted using DOE information systems.

- **Unclassified Computer Systems**
  Unclassified computer systems must not be used to process classified information. Classified information must be processed ONLY on accredited information systems in a designated security area, such as a Limited Area. UCI must be processed according to site level requirements.

- **Cyber Security and E-mail Attachments**
  There are some basic principles to follow when using email systems at work. Handle emails from an unknown source cautiously. Ensure the sender is a reliable source before clicking on a link embedded in the email. Do not open emails from a suspicious source, delete them.

Telephone numbers for the IT Help Desk at each site are listed in the Resource Library.

Section 4: TSCM, OPSEC and Cyber Security Quiz

1. The TSCM Program is an electronic counterintelligence program designed to detect, deter, isolate and nullify technical penetrations and technical security hazards.

   a. True
   b. False

2. I can be proactive in OPSEC by:

   a. Practicing need-to-know.
   b. Not discussing Unclassified Controlled Information (UCI) or classified information in public areas.
   c. Being aware of possible ways in which an adversary can collect information in an open environment (overheard conversations, notes left in open vehicles, etc.).
   d. All of the above.

3. If you receive a suspicious email, you should open it so see where it came from.

   a. True
   b. False

Section 5: Unclassified Controlled Information (UCI)

This section will focus on UCI.

What is UCI?

Who can access UCI?

How to protect UCI?

Where to store UCI?

Whom to contact?

Unclassified Controlled Information

UCI is broadly defined as information that may be exempt from public release either by statute, or under the Freedom of Information Act (FOIA) and for which disclosure, loss, misuse, alteration, or destruction would adversely affect national security or government interests.

UCI includes, but is not limited to:

1. **Official Use Only (OUO)**
    a. Personally Identifiable Information (PII)
    b. Export Control Information (ECI)
2. **Unclassified Controlled Nuclear Information (UCNI)**

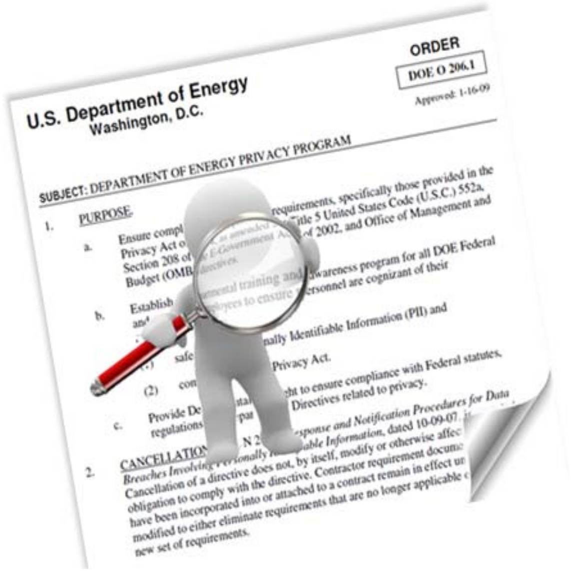
Unclassified Controlled Information

To be identified as **OUO**, information must be unclassified and meet both of the following criteria:

- Has the potential to damage governmental, commercial, or private interests if disseminated to persons who do not "need to know" the information to perform their jobs or other DOE-authorized activities.
- Fall under at least one of eight FOIA exemptions (exemptions 2 through 9). Information under Exemption 1 can never be OUO because it covers information classified by Executive Order. As of March 2011, Exemption 2 now only applies to information that relates solely to internal personnel rules and practices of an Agency. The scope of exemption 2 has been significantly reduced. See your Classification Officer for more details.

Requirements for identification, protection and control of OUO are located in DOE O 471.3.

Unclassified Controlled Information



U.S. Department of Energy
Washington, D.C.

ORDER
DOE O 206.1
Approved: 1-16-09

SUBJECT: DEPARTMENT OF ENERGY PRIVACY PROGRAM

1. PURPOSE.

a. Ensure compl requirements, specifically those provided in the Privacy Act o as amended Title 5 United States Code (U.S.C.) 552a, Section 208 of the E-Government Act of 2002, and Office of Management and Budget (OMB directives.

b. Establish mental training and awareness program for all DOE Federal and ployees to ensure personnel are cognizant of their

nally Identifiable Information (PII) and

(1) safe Privacy Act.

(2) con ght to ensure compliance with Federal statutes,

c. Provide De ta Directives related to privacy. regulations par

2. CANCELLATION N 2 esponse and Notification Procedures for Data *Breaches Involving Personally Identifiable Information*, dated 10-09-07. Cancellation of a directive does not, by itself, modify or otherwise affec obligation to comply with the directive. Contractor requirement docume have been incorporated into or attached to a contract remain in effect ur modified to either eliminate requirements that are no longer applicable new set of requirements.

One type of **OUO** information you may encounter is **Personally Identifiable Information (PII).**

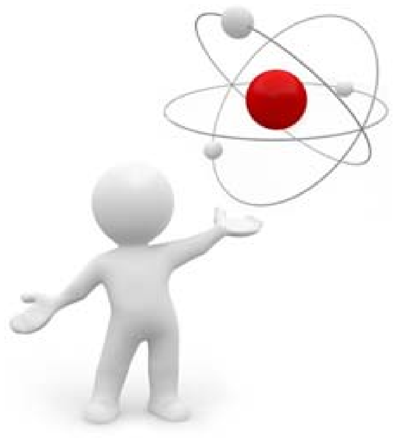
(PII is marked and protected as OUO, Exemption 6, Personal Privacy)

PII is any information maintained by DOE, contractors or subcontractors, about an individual including but not limited to:

- Education
- Financial transactions
- Medical history
- Criminal or employment history
- Information that can be used to distinguish or trace an individual's identity, such as his/her name, social security number, date of birth, place of birth, mother's maiden name, biometric data, etc.

Requirements for identification of PII are located in DOE O 206.1.

Unclassified Controlled Information



Another type of **OUO** information is **Export Control Information (ECI).**

(ECI is marked and protected as OUO, Exemption 3, Statutory Exemption. The ECI admonishment must appear adjacent to the OUO admonishment on the first page).

ECI is defined as unclassified technical information whose export is subject to export control and whose unrestricted public dissemination could help proliferants or potential adversaries of the US.

All nuclear technologies and most other technologies are controlled by the US with respect to foreign nationals-both those in and out of the US Requirements for identification, protection and control of ECI are located in *US DOE Guidelines for Export Control and Nonproliferation dated July 1999*.

Unclassified Controlled Information

Unclassified Controlled Nuclear Information (UCNI) is certain unclassified information that has been determined to fall under the purview of the following Atomic Energy Commission programs:

- Nuclear material production
- Safeguards and Security
- Nuclear weapons design

UCNI is protected by law and implemented within DOE through 10 CFR part 1017 and DOE Order 471.1B. UCNI protects against providing an adversary with easy access to information that has the potential to damage our government and therefore must be protected.

Controlling Access to UCI

A person granted routine access to UCI must have a **need to know** the specific information in the performance of official or contractual duties. Because UCI is unclassified, **a security access (L or Q) is not required**; however, recipients must be **advised of the protection requirements**. Unless specifically authorized, foreign nationals are not allowed access to ECI and UCNI.

STORAGE - UCI must be protected at all times from unauthorized disclosure. UCI must be stored in a locked room or locked receptacle with the key controlled only by individuals meeting the need-to-know criterion. In a Limited, Exclusion, or Material Access Area, UCI must be stored to prevent unauthorized access.

REPRODUCTION - UCI may be reproduced without permission of the originator. Reproduction shall be limited to the minimum number of copies necessary consistent with the need to carry out official duties. Reproduced copies shall be marked and protected in the same manner as the original document. Copy machine malfunction must be cleared with all paper paths checked for UCI material.

Transmission of UCI

- **Transmission by Email:**
  UCI must be encrypted when electronically transmitted outside the site's network. Encryption can be accomplished by using Entrust for email or other encryption software available at your site. Electronic transmission of UCNI must be encrypted.

- **Transmission by Fax:**
  When faxing UCI (excluding UCNI which must be sent via a secure telephone facsimile), the sender must contact the recipient prior to faxing the UCI document. The sender is responsible for making a follow-up call to confirm that the entire UCI document was received.

- **Transmission by Mail Offsite:**
  Place documents in a sealed opaque envelope or wrapping. Stamp or write the words: To Be Opened by Addressee Only. The document can be mailed First Class, Express, Certified or Registered Mail, or sent via any commercial carrier.

- **Transmission by Mail Onsite:**
  Place in a sealed, opaque envelope or wrapping. Stamp or write the words:
  To Be Opened by Addressee Only.

  Additional information regarding the protection requirements for UCI and telephone numbers for UCI contacts is located in the Resource Library.

Section 5: Unclassified Controlled Information Quiz

1. Given the need to know, who can have access to Unclassified Controlled Information?

    a. Uncleared and cleared employees.
    b. Uncleared employees only.
    c. Cleared employees only.
    d. None of the above.

2. Unclassified Controlled Information (UCI) must be protected from unauthorized disclosure.

    a. True.
    b. False.

Section 6: Hosting Foreign National Guests

DOE is a world leader in advancing new technologies requiring scientific and technical collaboration with foreign nationals. Hosting foreign nationals at DOE facilities and/or discussing DOE information require multiple subject matter expert reviews and approval by an authorized approval authority. Hosting requirements are in **DOE Order 142.3A Unclassified Foreign Visits and Assignments Program.** If hosting foreign nationals in support of DOE business operations, onsite or offsite, your site visitor control representative can provide detailed documentation and approval guidance.

Hosting Requirements:

Hosts are responsible for ensuring adherence to DOE and site requirements including personnel security and counterintelligence reporting requirements. Hosts must have sufficient knowledge of the work being performed so that they can provide guidance regarding the limitations of the visits. In some cases, a designated individual must physically escort foreign nationals. If required, this must be specified in the security plan provided by the security organization at the sponsoring site.

Hosting Foreign National Guests: Preparing for the Visit

- Complete the foreign national guest access request documentation and submit to your site foreign visitor representative.
- Contact your local counterintelligence office to assist with the completion of the host briefing.
- Determine the areas of your work that may be sensitive and plan for appropriate protective measures.
- Review and become familiar with the Sensitive Subjects List to better understand restrictions on foreign national access. (For questions concerning the Sensitive Subjects List contact your local export control contact.)
- Assess whether discussion of selected unclassified information with foreign nationals could divulge proprietary details related to Cooperative Research and Development Agreements (CRADAs) or other collaborative programs or projects.
- Brief staff who will be working with the foreign national. Inform them of the areas approved for the foreign national to access and the scope of technical issues approved for discussion or research.

Hosting Foreign National Guests: Your Responsibilities

Ensure visas, passports, and work authorizations are appropriately validated upon arrival and that the foreign national is informed of the following:

- The terms and conditions of access approval, including restrictions and requirements to notify you, the host, of changes in name or status information.

- The requirement to notify you of any civil or criminal problems that could affect his/her status and association with DOE. The failure to provide appropriate documentation when required or providing fraudulent documentation will result in suspension of access approval, removal from your site, and possible cancellation of future access.

Hosting Foreign National Guests: Reporting Requirements

Be alert to indications that foreign nationals might be collecting information on the basis of intelligence tasking, or might be an intelligence officer. Foreign intelligence services often foster professional and personal relationships as a means to elicit or otherwise obtain desired information.

In view of that, the DOE Headquarters Office of Intelligence and Counterintelligence has implemented reporting requirements, which include information about your professional, personal, and financial relationships with citizens of sensitive countries. Also, in the event you become aware of suspicious activity, you are required to report activity to your local counterintelligence office as noted in Section 7 of this briefing.

Hosting Foreign National Guests: Closing out the Visit

- Contact your site foreign national access coordinator in accordance with your local site procedures to ensure 15-day closeout in the Foreign Access Central Tracking System (FACTS).

- **For additional information or answers to questions concerning your host responsibilities, contact your site's Foreign Visitor coordinator.**

- Remember: As the host, you are personally responsible for maintaining the security of the access and for precluding the inadvertent or unintentional passage of unauthorized information.

Telephone numbers for questions regarding hosting foreign nationals are listed in the Resource Library.

Section 6: Hosting Foreign National Guests Quiz

1. In order to be a Host of a Foreign Guest you must have:

   a. Received Host Training from the Office of Counterintelligence.
   b. Be a Federal Employee.
   c. Must have held a Q or L clearance for the past 5 years.

2. If you have been designated and received the appropriate training to be a "Host of a Foreign Guest" you must:

   a. Be familiar with the DOE Sensitive Subject List.
   b. Ensure visas, passports, and work authorizations are appropriately validated.
   c. Have sufficient knowledge of the work being performed.
   d. All of the above.

Section 7: Counterintelligence

(This section is furnished by the DOE Office of Counterintelligence, Oak Ridge Field Office (ORFO). All questions on this topic should be directed to the ORFO at (865) 241-0233.)

The Foreign Intelligence Threat - DOE/NNSA and its contractors are the guardians of some of our nation's most closely held and vital secrets, products, and technology. As such we are targets of extreme interest by foreign powers seeking to acquire those secrets.

The information you hold as a member of the workforce is valuable to almost any foreign intelligence service in the world. It is not necessary for you to hold a security clearance or work with classified information for you to be of interest to an intelligence agency. Foreign Intelligence Services want to know everything about what we are doing and how our facilities function, so that they can exploit that information.

All potential espionage or terrorism related concerns should be promptly reported to the ORFO at
(865-241-0233). Visit the ORFO Website (See Resource Library) for specific program information, detailed reporting requirements, foreign travel and visit information, and more!

Intelligence Collection

To obtain needed information from foreign countries, governments maintain professional intelligence and security services - almost every country has them.

Intelligence organizations task their employees, and sometimes private citizens, to collect US information of value.

Valued information sought after includes:

- Military/defense (classified information)
- Political
- Economic
- Science/technology (even if later published, to get a head start)
- Business (sensitive, proprietary, intellectual property)

Traditional collection methods still use foreign agents, traitors, listening devices, and satellite surveillance, but in today's environment, we must also be alert to the more overt methods of collection, such as those listed below.

> Events, such as international conferences, conventions, and trade fairs, attract foreign scientists and engineers, providing foreign intelligence collectors a group of specialists on a key topic of interest. In addition to obtaining available literature, intelligence collectors use these opportunities to elicit information and identify personnel who can be targeted for further contact.
>
> Research activities may be exploited during foreign travel, while hosting foreign visitors or assignees, or by other means of international collaboration or joint ventures.

Counterintelligence Reporting

To ensure DOE/NNSA assets (people, information, and resources) are protected from foreign intelligence gathering efforts, employees are required to report the following counterintelligence information:

Unusual Solicitations

- Attempts by ANY unauthorized persons to gain access to classified information.
- Situations that appear to be attempts by foreign intelligence services to enlist cooperation.
- Inquiries regarding sensitive or classified information about your workplace, your official responsibilities, and/or activities and/or identities and activities of coworkers.
- Contact with foreign nationals who make requests or statements that could be attempts at exploitation or elicitation.
- Indicators of "Insider Threat".

Anomalies

A foreign power activity or knowledge, inconsistent with the expected norm that suggests foreign knowledge of US national security information, processes, or capabilities.

Contact with Foreign Nationals

Professional, personal, and financial relationships with citizens of sensitive countries. This includes relationships that are maintained via the internet (i.e., email, chat rooms, social networking sites, internet dating, etc).

Foreign Travel

- All personnel (both cleared and uncleared) must attend a Counterintelligence Pre-Travel Briefing prior to traveling to Sensitive Countries (includes both business AND personal travel).
- Travel to Non Sensitive Countries generally DOES NOT require a briefing, unless Sensitive Subjects or sensitive country nationals are involved.

The Insider Threat

Risk of betrayal of trust does not depend upon the presence of a foreign adversary. It depends only upon an insider with the opportunity to betray, some combination of character weaknesses and situational stresses, and a trigger that sets the betrayal in motion. The insider is a major threat to national security, using his or her access to programs, systems, people and facilities, and knowledge of security protocols to obtain information.

As a general rule, the four pre-conditions described below must be present before a disaffected or troubled employee commits a serious betrayal of trust like espionage.

- Ability to Overcome Inhibitions such as moral values, fear of being caught, and loyalty to employer or co-workers.
- Trigger - Something that sets the betrayal in motion.
- Motive or a need to be satisfied through the crime.
- Opportunity to commit the crime.

The Insider Threat

There is no established formula for recognizing that someone is involved in espionage; however, certain situational factors or suitability issues can make an individual predisposed to volunteer or make them vulnerable to exploitation by foreign intelligence officers.

- **Behavioural and Suitability Issues:**
  - Substance abuse or dependence
  - Hostile, vindictive, or criminal behavior
  - Extreme, persistent interpersonal difficulties
  - Unreported foreign interaction
  - Gamblers/Lavish spenders
- **Socio-Economic Factors:**
  - Global market is expanding
  - Increased foreign interaction
  - Vulnerabilities (i.e., financial crisis)
  - Organizational loyalty is diminishing
  - Ethnic or religious ties
  - Moral justification
- **Psychological Factors:**
  - Narcissistic personality - i.e., a grandiose sense of their own importance – a sense of entitlement.
  - Sociopathic personality - i.e., lacking a sense of moral responsibility or social conscience.
- **Technological Trends** - Developments in information technology make it much harder to control the distribution of information

Potential Indicators of Espionage Activities

Your role as an employee is to be aware of potential espionage indicators and to report your concerns to the ORFO. In some cases your concerns might be based on a feeling that "something just isn't right." As a general rule, if it doesn't seem right, it probably isn't and, therefore, should be reported. Working together, we can identify issues earlier, render assistance before the situation becomes irreversible, and ultimately protect the security of our mission.

- Disgruntlement
- An "above-the-rules" attitude
- Risk-taking behaviors
- Repeated impulsive behaviors
- Willingness to violate the rights of others to achieve one's own ends
- Conflicting loyalties to US Government
- Willingness to break rules or violations of laws and regulations
- Membership in any group that advocates the use of force or violence to cause political change within the US

Potential Indicators of Espionage Activities

- Statements or actions indicating an abnormal fascination with "spy" work
- Attempts to gain unauthorized access to classified or sensitive information
- Undue curiosity or requests for information about matters not within the scope of the individual's job or need-to-know
- Unauthorized removal of classified information
- Unusual work schedules
- Unexplained affluence
- Extensive use of copy, facsimile, or computer equipment which may exceed job requirements
- Frequent short trips to foreign countries or within the US to cities with foreign diplomatic facilities, for unusual or unexplained reasons
- Unreported foreign travel
- Unreported foreign contacts
- Joking or bragging about working for a foreign intelligence service
- Behavior indicating concern that one is being investigated or watched, such as actions to detect physical surveillance
- Attempt to conceal any activity covered by one of these counterintelligence indicators

"If you want to do these people a favor who have problems - and I'm talking from experience, say something. If somebody had said something to me and put a block in front of me and said 'I think Jeff's got a problem and I don't think that he's handling it very well,' that would have been enough to stop the process." -- Jeffrey Carney (US Air Force, convicted spy)

Congratulations!

You have completed the Oak Ridge Office Annual Security Refresher Briefing.

Please continue to view your Briefing Summary Record. A copy of this record will be emailed to you and the appropriate security official.

Briefing Summary Record

Below is a summary of today's briefing.

Briefing Module:
User's Name:
Email:
Completion Date:

Answers to Quizzes

Section 1: Security Badges and Identification of Prohibited and Controlled Articles Quiz

1. The following articles are prohibited on DOE property.

   - The answer is d. All of the above

2. The following items are controlled articles.

   - The answer is d. All the above

Section 2: Reporting Requirements and IOSC Quiz

1. Which of the following events are reportable within 2 working days of the event?

   - The answer is c. Arrests, criminal charges, bankruptcy.

2. Marriage or cohabitation with a person in a spouse-like relationship must be reported within 45 days.

   - The answer is TRUE.

3. Waste, fraud and abuse only has to be reported if a crime is involved.

   - The answer is FALSE.

4. When does an "incident of security concern" occur?

   - The answer is a. Any time there is a potential or actual compromise of classified or Unclassified Controlled Information (UCI) or when a security rule is violated.

Section 3: Classified Information Quiz

1. Classified matter is structured into which three categories?

- The answer is b. National Security Information, Formerly Restricted Data and Restricted Data are the three categories of classified information.

2. Documents or material in a classified subject area intended for Congress does not have to be reviewed by a DC.

- The answer is a. False.

3. What must an individual possess before being allowed access to classified matter?

- The answer is c. Appropriate access authorization, need to know and a signed Classified Information Non-disclosure Agreement (SF-312).

4. The classification levels are:

- The answer is d. All of the above.

Section 4: TSCM, OPSEC and Cyber Security Quiz

1. The TSCM Program is an electronic counterintelligence program designed to detect, deter, isolate and nullify technical penetrations and technical security hazards.

- The answer is a. TRUE.

2. I can be proactive in OPSEC by:

- The answer is d. All of the above.

3. If you receive a suspicious email, you should open it so see where it came from.

- The answer is b. FALSE.

Section 5: Unclassified Controlled Information Quiz

1. Given the need to know, who can have access to Unclassified Controlled Information?

    - The answer is a. Uncleared and cleared employees.

2. Unclassified Controlled Information (UCI) must be protected from unauthorized disclosure.

    - The answer is TRUE.

Section 6: Hosting Foreign National Guests Quiz

1. In order to be a Host of a Foreign Guest you must have:

    - The answer is a. Received Host Training from the Office of Counterintelligence.

2. If you have been designated and received the appropriate training to be a "Host of a Foreign Guest" you must:

    - The answer is d. All of the above.